



***Cabinet for Health and Family Services (CHFS)  
Information Technology (IT) Policy***



**065.022 Kentucky Online Gateway (KOG)  
Role Recertification Policy**



**Version 1.0  
October 25, 2018**

<a href="#">065.022 KOG Role Recertification Policy</a>	Current Version: 1.0
065.000 Application Development	Review Date: 10/25/2018

## Revision History

Date	Version	Description	Author
10/25/2018	1.0	Effective Date	CHFS OATS Policy Charter Team
10/25/2018	1.0	Review Date	CHFS OATS Policy Charter Team
10/25/2018	1.0	Revision Date	CHFS OATS Policy Charter Team

## Sign-Off

Sign-off Level	Date	Name	Signature
Executive Advisor (or designee)	10/25/2018	Bernard Decker	
CHFS Chief Information Security Officer (or designee)	10/25/2018	Dennis E. Leber	

<a href="#">065.022 KOG Role Recertification Policy</a>	Current Version: 1.0
065.000 Application Development	Review Date: 10/25/2018

## Table of Contents

<b>1</b>	<b>POLICY DEFINITIONS.....</b>	<b>4</b>
<b>2</b>	<b>POLICY OVERVIEW.....</b>	<b>6</b>
2.1	PURPOSE .....	6
2.2	SCOPE .....	6
2.3	MANAGEMENT COMMITMENT.....	6
2.4	COORDINATION AMONG ORGANIZATIONAL ENTITIES .....	6
2.5	COMPLIANCE .....	6
<b>3</b>	<b>ROLES AND RESPONSIBILITIES .....</b>	<b>7</b>
3.1	CHIEF INFORMATION SECURITY OFFICER (CISO) .....	7
3.2	CHIEF PRIVACY OFFICER (CPO) .....	7
3.3	SECURITY/PRIVACY LEAD .....	7
3.4	CHFS CONTRACT, STATE, AND VENDOR STAFF/PERSONNEL .....	7
3.5	SYSTEM DATA OWNER AND SYSTEM DATA ADMINISTRATORS.....	7
3.6	ORGANIZATIONAL/SYSTEM ADMINISTRATOR .....	8
<b>4</b>	<b>POLICY REQUIREMENTS .....</b>	<b>8</b>
4.1	GENERAL .....	8
<b>5</b>	<b>POLICY MAINTENANCE RESPONSIBILITY .....</b>	<b>8</b>
<b>6</b>	<b>POLICY EXCEPTIONS .....</b>	<b>9</b>
<b>7</b>	<b>POLICY REVIEW CYCLE.....</b>	<b>9</b>
<b>8</b>	<b>POLICY REFERENCES .....</b>	<b>9</b>

<a href="#">065.022 KOG Role Recertification Policy</a>	Current Version: 1.0
065.000 Application Development	Review Date: 10/25/2018

# 1 Policy Definitions

- **Access:** The ability to use or modify an information resource.
- **Application:** A software program designed to perform a specific function (e.g., Benefind, Worker Portal, etc.).
- **Confidential Data:** COT standards define confidential data as the data the Commonwealth has a legal obligation to not disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Contract Staff/Personnel:** An employee hired through a state approved (i.e. System Design/Development Services {SDS} Vendor Agreement/Company) vendor who has a master agreement with the state.
- **Electronic Personal Health Information (ePHI):** Any protected health information (PHI) that is covered under Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred, or received in an electronic form.
- **Federal Tax Information (FTI):** Information received from the Internal Revenue Service (IRS) or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service, that includes tax information. Examples would be an individual's tax return or anything that the IRS collects and that the IRS is going to use in order to determine a person's tax liability or potential tax liability.
- **Personally Identifiable Information (PII):** Information that can be used to distinguish or trace an individual's identity (i.e. name, Social Security number, biometric records, etc.). PII can be the individual's personal information or is identified when combined with other personal or identifiable information (i.e. date of birth, birth place, mother's maiden name, etc.).
- **Recertification:** An ongoing process designed to validate whether continued access to a business application is required in order to complete assigned job duties.
- **Role:** Defines the user's access within an Application.
- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)
- **State Staff/Personnel:** An employee hired directly through the state within the CHFS.

<a href="#">065.022 KOG Role Recertification Policy</a>	Current Version: 1.0
065.000 Application Development	Review Date: 10/25/2018

- **System/Data Administrator:** An individual who is responsible for the data administration process by which data is monitored, maintained, and managed. This person is responsible for controlling application data assets, as well as their processing and interactions with different applications and business processes. This person is also tasked with access management to the system/data using the Role-based Access Control (R-BAC) model. In the Cabinet for Health and Family Services this role is generally played by a CHFS Branch Manager.
- **System/Data Custodian:** An individual who is responsible for the maintenance and protection of the data. This role is usually filled by the IT department, which owns the Infrastructure. The duties include performing regular backups of the data, implementing security mechanisms, periodically validating the integrity of the data, restoring data from backup media, and fulfilling the requirements specified in the enterprise security policies, standards, and guidelines that pertain to information security and data protection. In the Commonwealth of Kentucky this role is generally played by Commonwealth Office of Technology (COT).
- **System/Data Owner:** The person who has final agency responsibility of data protection and is the person held liable for any negligence when it comes to protecting the specific application's data/information assets. This role/person is the owner of the system that holds the data, usually a senior executive, designates the confidentiality of the system/data, and assigns the data admin, and dictates how the information should be protected based on business' policies. In the Cabinet for Health and Family Services this role is generally played by a CHFS Business Executive.
- **Vendor Staff/Personnel:** An employee contracted through an approved Master Business Associate Agreement, or other formal agreement, to provide temporary work for CHFS.
- **Worker Type:** Logical containers in which workers are grouped, based on the application access required and the type of work that they perform in order to fulfill their job responsibilities.

<a href="#">065.022 KOG Role Recertification Policy</a>	Current Version: 1.0
065.000 Application Development	Review Date: 10/25/2018

## 2 Policy Overview

### 2.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish a comprehensive level of security controls through role recertification guidelines within the Kentucky Online Gateway (KOG). This document establishes the agency's Role Recertification, which helps manage risks and provides guidelines for privacy and security best practices regarding the ongoing security management of roles through recertification for access to applications housed in KOG.

### 2.2 Scope

The scope of this policy applies to all internal CHFS state, contract, and vendor staff/personnel, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems.

### 2.3 Management Commitment

OATS Division Directors, the CHFS Chief Technical Officer (CTO), Chief Information Security Officer (CISO), and IT Executive Management have reviewed and approved this policy. Senior Management supports the objective put into place by this policy. Violations of not abiding by this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. CHFS shall report illegal activities or theft of CHFS property (physical or intellectual) to the appropriate authorities.

### 2.4 Coordination among Organizational Entities

OATS coordinates with CHFS organizations and/or agencies that access applications, systems, and facilities. All organizational entities that interact with CHFS are subject to follow requirements outlined within this policy.

### 2.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in applicable state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Additionally, applicable agencies follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

<a href="#">065.022 KOG Role Recertification Policy</a>	Current Version: 1.0
065.000 Application Development	Review Date: 10/25/2018

## 3 Roles and Responsibilities

### 3.1 Chief Information Security Officer (CISO)

Individual responsible for providing guidance and direction in assessment, planning, and implementation of all security standards, practices, and commitments required. This individual is responsible for adherence to this policy.

### 3.2 Chief Privacy Officer (CPO)

An individual responsible for overseeing activities related to the development, implementation, maintenance of, and adherence to the Cabinet's and Commonwealth's information privacy and confidentiality policies and procedures in compliance with federal and state laws. This individual will conduct Health Insurance Portability and Accountability Act (HIPAA) risk analysis through coordination with the Information Security Agency Representative, the CISO, or CHFS OATS Information Security (IS) Team, and other CHFS agencies, and will ensure compliance with HIPAA notification and reporting requirements in the event of an identified breach.

### 3.3 Security/Privacy Lead

Individual(s) designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate staff/personnel. This individual(s) is responsible for providing privacy and security guidance and direction for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff/personnel. This role along with the CHFS OATS IS Team is responsible for adherence to this policy.

### 3.4 CHFS Contract, State, and Vendor Staff/Personnel

All CHFS contract, state, and vendor staff/personnel must adhere to this policy. All staff/personnel must comply with referenced documents, found in section [8 Policy References](#) below that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

### 3.5 System Data Owner and System Data Administrators

Management/lead who works with the application's development team, to document components that are not included in the base server build, and ensures that functionality and backups are conducted in accordance with business needs. This individual(s) is also responsible for working with personnel within the enterprise, agency, application, technical and business areas, for providing full recovery of all application functionality, as well as meeting federal and state regulations for disaster recovery situations.

<a href="#">065.022 KOG Role Recertification Policy</a>	Current Version: 1.0
065.000 Application Development	Review Date: 10/25/2018

### **3.6 Organizational/System Administrator**

KOG personnel that are defined with a management/lead role, who work with the application's development team, to control data assets and business processes through R-BAC, in order to meet the guidelines set by federal and state regulations.

## **4 Policy Requirements**

### **4.1 General**

The purpose of this policy is to ensure that a KOG application role assigned to a user is relevant to their current job duties. Based on the user's worker type and job duties, roles are assigned when they are granted application access by their Organization/System Administrator. A user's job duties may change, but their worker type may remain the same, which could result in application access that is no longer required for their new duties.

Organization/System Administrators determine if a user's role is required based upon recertification. User access in roles (i.e. FTI – View Only) can be revoked at the time of recertification, by the Organization/System Administrator, without having to complete an individual KOG action on each user. Recertification dates can be set to a specified number of days (i.e. 180 days), or by a specific day/month (i.e. 15<sup>th</sup> of June). These roles cannot be recertified if within twenty (20) days of the next recertification date.

Questions regarding recertifications can be submitted via email to the [KOGHelpdesk@ky.gov](mailto:KOGHelpdesk@ky.gov).

## **5 Policy Maintenance Responsibility**

The OATS IS Team is responsible for the maintenance of this policy.



<a href="#">065.022 KOG Role Recertification Policy</a>	Current Version: 1.0
065.000 Application Development	Review Date: 10/25/2018

## 6 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

For any staff located within the Department for Behavioral Health, Development, and Intellectual Disabilities (BHDID) who are not on boarded or utilizing KOG, the COT F181EZ Form shall be used to request any action (create, modify, or delete) related to CHFS domain accounts/access. Once forms are completed and approved, they must be submitted to [CHFSServiceRequests@ky.gov](mailto:CHFSServiceRequests@ky.gov) for completion. Please refer to the COT Forms Page for instructions and more detailed information.

## 7 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

## 8 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- Enterprise IT Form Instructions: F181EZ- Staff Service Request, EZ Version, Form Instructions
- Enterprise IT Form: F181EZ- Staff Service Request, EZ Version, Form
- Enterprise IT Form Instructions: F181i- Staff Services Request Form Instructions
- Enterprise IT Form: F181- Staff Service Request Form (and COT Entrance/Exit Form)
- Enterprise IT Form: F085- Security Exemption Request Form
- Internal Revenue Services (IRS) Publications 1075
- Kentucky Online Gateway (KOG)
- Kentucky Revised Statute (KRS) Chapter 61.878 Certain public records exempted from inspection except on order of court – Restriction of state employees to inspect personnel files prohibited
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Security Information